

security measure that verifies, via an individual PLS, where the IA is located. Essentially, if the IA requiring access at a given place (*e.g.* a website or bank account) has coordinates that do not coincide with those that were obtained from the individual PLS, then the IA may be considered to be intrusive.

5 As a security measure, the IA that requires access to a particular site, service or operation will require an associated individual PLS. When the IA identifies itself to the security system (*e.g.*, entering an identification number in an ATM [automatic teller machine]), the security system will preferably sends a request to the central PLS to verify where thy IA with the corresponding (entered) "identity" is located. The central PLS
10 thence preferably communicates with the individual PLS associated with the all IA's bearing that "identity". Accordingly, the central PLS system will become apprised of the exact location of a candidate set of individual PLS's. The central PLS then preferably sends these coordinates to the security system. Preferably, the security system will then compare the coordinates that are obtained over the network from individual PLS's with
15 the coordinates of the system where the IA is located and that requested access. (The coordinates of the IA that requested access can be obtained, from the location of the input arrangement used by the IA attempting access, for instance, the location of an ATM being operated.) If the coordinates do not match then the request for access is rejected.

possible locations at which the registered intelligent agents may gain access; and a threshold manager which permits access, to a given location, of an entry intelligent agent that corresponds to at least one intelligent agent in the general register.

In another aspect, the present invention provides a method of authenticating an intelligent agent, the method comprising the steps of: ascertaining the location and identity of an entry intelligent agent attempting to gain access to the location, the identity being ascertained via an identification tag associated with the intelligent agent; providing a general register of identification tags corresponding to a plurality of intelligent agents and of possible locations at which the registered intelligent agents may gain access; and permitting access, to a given location, of an entry intelligent agent that corresponds to at least one intelligent agent in the general register.

Furthermore, in another aspect, the present invention provides a program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for authenticating an intelligent agent, the method comprising the steps of: ascertaining the location and identity of an entry intelligent agent attempting to gain access to the location, the identity being ascertained via an identification tag associated with the intelligent agent; providing a general register of identification tags corresponding to a plurality of intelligent agents and of possible

network on whether there is an IA with a certain identification number. These special measures can include, for example, cellular telephones that are capable of sending wireless signals to local cellular providers that themselves are connected to global networks or to powerful broadcasting stations that can send signals far away (to satellites or other servers) with information regarding the location of IA's. A general PLS is schematically illustrated in Fig. 3 and will be discussed in more detail further below.

Preferably, the "embedded" devices that are located on a person, such as watches, telephones, digital wallets etc. (104) and that contain a PLS, can, at a given time, be in an active mode or a passive mode. In the active mode, device 104 will be connected to a network (e.g., via wireless measures) and can receive an IA. In the passive mode, they are not receiving any signals from a network. The embedded devices can periodically go into active mode to download some data from global networks. They can receive an IA and then disconnect from network. To detect such an IA, it is desirable to equip embedded devices with a PLS that can receive and send signals regardless of whether embedded devices are in passive or active mode.

In one embodiment of the present invention, a PLS can include a GPS arrangement that would allow for precisely identifying the position of a device in which a GPS is located. Such an exact identification of position may be needed since the local server

any case, there is no signal sent out from the GPS receivers. They know where they are relative to the GPS satellites, which are all in known spatial coordinates.

The precise identification of IA's (or, more particularly, of the devices in which they are located) may be needed since there can be several IA's (some of which are
5 intrusive) with the same identification numbers in the proximity of a local cellular provider (but located in different devices). By combining a GPS with measures to send their location to a server, a PLS is realized.

As shown in Figure 2, a method of verifying user identity may include several steps. First (200), an IA may provide its identification number by communicating with a
10 server or embedded device to the effect that performance of a particular operation, or entry into a particular entity, is desired.

Then (201), the IA identification number is preferably sent to the database to verify whether any IA with that identification number belongs to the service that uses the PLS in question.

15 Next (202), the IA identifies its location (for instance, by identifying a location of a local cellular provider that is linked to a computer system into which the IA wants to enter, or by utilizing a GPS subsystem in the PLS).

step 210, a determination is made as to whether the two positions coincide. If yes, access is allowed (212), while if no, access is rejected (211).

As to running a comparison in step 207, the exactness required of the match may depend on several factors, including the type of services that the IA requested. For example, if the IA requests access to an ATM, then it would likely merely suffice if the location of the IA can be defined at a level of precision sufficient to distinguish between the location of the ATM at hand and that of the nearest other ATM. However, if there are, for example, two ATM's near a cellular provider and both ATM's receive requests for access from IA's within a short period of time, and if the location of the IA in this instance is defined only in terms of the cellular provider that receives the strongest signal from the IA, then at that level of precision (in locating an IA), it might not be clear as to whether two different IA's have requested access to two different ATM's or if the same IA requested access to the two IA's in relatively quick succession. In this case, it may be warranted to include a more precise measure for ascertaining IA locations, such as a GPS, that could be used as a supplement.

Another possible criterion for permitting or denying access of an IA to a given location may be time-based. Particularly, an IA could be denied access to a given location or locations if it is ascertained that the IA has requested access two different locations

open systems interconnection (OSI). Figure 4 thus illustrates how novelty segregation module features can fit OSI architecture.

The OSI typically includes seven layers - physical link, data link, networking, transport, session, presentation, application (400 - 406, respectively). A description of these layers functions can be found in Gill Waters, "*Computer communication networks*", 1991, McGraw-Hill Book Company, England.

Concerning the manner in which OSI architecture can preferably be related to some IA authentication features, in accordance with an embodiment of the present invention, the IA interacts with a protocol 407 that can be located in physical communication devices (like modems) and therefore is linked to physical link layer 400, as shown in Fig.4.

The module 410 that operates with a flow of bits and represents a stream of bits as 1's and 0's can preferably read the identification IA number. This module 410 can be located in the data link layer 501 that processes bit streams from data communication link. Another possible location of module 410 is a buffer in a transport layer 404, since the transportation block provides a flow control and contains buffer where bits from communication links are accumulated. Similarly, the reading of an IA identification number could be undertaken in a presentation layer 401.

